IMAGE PROCESSING FOR FORENSIC INVESTIGATION

SHORT SYNOPSIS

Submitted in partial fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

to

Manav Rachna International Institute of Research and Studies
(Deemed to be University)

by

Monika
Registration number: 16/Ph.D/036

Under the supervision of
Dr. Dipali Bansal
Professor, FET, MRIIRS

FACULTY OF ENGINEERING AND TECHNOLOGY

MANAV RACHNA INTERNATIONAL INSTITUTE OF RESEARCH & STUDIES

SECTOR-43, SURAJKUND –DELHI ROAD, FARIDABAD – 121001

FACULTY OF ENGINEERING AND TECHNOLOGY

Certificate

I hereby declare that the short synopsis "Image Processing for Forensic Investigation"being submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy inECE Department under faculty of engineering and technology of Manav Rachna International Institute of Research & Studies, Faridabad during the academic year 2016.

It is a bona fide record of original work carried out under the supervision of Dr. Dipali Bansal and has not been submitted in full or part to any other university or institute for degree or diploma. Further, it is certified that short synopsis is plagiarism free and proof has been submitted.

Monika
16/Ph.D/036

Signature of the Supervisor

Dr.Dipali Bansal
Professor(ECE Department)
FET,MRIIRS

(Chairman, DRC)

Chairperson, CDP

ABSTRACT

Forensics Science helps in exploring the forensics investigation of digital era which provides mandatory information and innovative techniques for forgery detection. In today's digital world image tampering were done easily by youth for getting good carear settlement in life without any efforts. Digital Image Processing is emerging as a new field and finds mention in many electronic and computer applications. Forensics Image Processing aims to secure digital communications like online transaction for surveillance supports, CCTV recording, banks data tempering, road accident scenes etc.

Forgery detection of images still having computational complexity in terms of Time and Space especially in small tampered regions where statistical measurement analysis for image integrity become difficult due to similar component used in forged regions. Image tampering software tool like Adobe Photoshop, Corel Paint Photoshop are available easily from free online resources at any time for the purpose of image manipulations. Therefore improvement of forgery detection speed is the main concern with the implementation of reduced computational complexity and testing can be applied on different formats of digital images in order to get better results.

Dataset of tampered images will be collected from online resources like MICC_F220, MICC_F600 etc. to test forged images using various existing transform techniques for originality and identifying exact location of forgery for optimizing forensic science investigation and also implement the findings on real time datasets.

Forgery detection of tampered images will be evaluated based on various parameters for artifact removal and compared with recent existing techniques. Image forgery detection algorithm will be developed for providing Quality of Services like Security, Accuracy, Reliability, computational complexity and real time implementations. Analysis of Image Processing for forensic investigation is proposed with the help of MATLAB programming software tool.

Key words: **Forensic Science, Digital Image forensics Analysis, Forensic Investigation, Matlab, R2011a.**

CONTENTS

S. No.	Description	Page No.
1	Introduction	1-2
2	Literature Review 2.1 Gaps in Literature	3-8
3	Description of Broad Area	9-13
4	Objectives of the Study 4.1 Problem formulation 4.2 Objectives	13-14
5	Methodology to be adopted 5.1 Evaluation parameters	14-15
6	Expected Outcome of the Research	16
7	Proposed Time Frame(Gantt Chart)	16
8	References	17-20

1. INTRODUCTION

Now a day's natural communication of data transmission isdone easily by online media like images, video and audios for digital communications. Sharing, storage, business, e-services like airline reservations, Internet commerce, telecommunications billing, electronic banking, transaction processing, credit cards, capital stock trading, life sciences research, health care claims processing and many more activities are performed in our daily life routine .Increasing dependencies of digital communication having challenges in protecting and managing information as securedcommunication. Tampering becomes easier due to easily available software. However authenticity of images and videos become faithless data (Garfinkel 2010). Digital image forensic approaches overcomes image tampering and aims to improve the image quality for today digital world by highlighting the need of new methods for originality and its quality. Knowledge of the image input source is important since it allows device knowledge for investigators need. Most common type of copy move tampering was widely utilized in digital transaction where a portion or some section of an image was tampered with similar features of the same image, which made difficult to estimate accurate location of forgeries.

Passive and Active forgery detection approaches are the two main branches of image forensic techniques. Active techniques have some limitations like need of specific cameras and human interventions. To overcome these limitation passive techniques wereutilized where it does not need prior information about images. Many methodologies for passive forgeries are identified and tracked by (Birajdar and Mankar 2013).

This research gives new directions to trace out the tampering detection that helps in finding the dedicated changes like statistical changes etc. Various digital image forensic detection techniques are discussed for future research and an attempt is made to implement new methodology for forgery detection. Passive approach includes different categories of feature extraction like block-based feature extraction techniques, key-point based featureextraction techniques and segmentation based feature extractiontechniques via differenttransform methodologies. These methodologies must be robust for all conditions of pre-processed and post-processed image processing explained by (Chauhan, Kasat, Jain and Thakare 2016).

Therefore this research would be focused on blind passivemethodologies in the Image forensics for detecting tamperedregion in digital images.Figure1 presents basic digital image forgery forensic approach that involve different feature extraction and matching process through optimized threshold parameters with digital image processing approaches and Figure3. Illustrate the Work Flow Chart of proposed research.

Motivation of the Study

1. Now a day's tampering of digital images is very easy due to easily available softwareeditingtools which always puts questions towards any types of image data.
2. One of the most popular research directions is image forensic science, provides main reason for research work in many applications for the purpose of Security, Quality, Validation and Reliability.
3. Existing methodologies of image forgery encourage forensic investigation to perform extensive research in this field for maintaining originality of digital images.

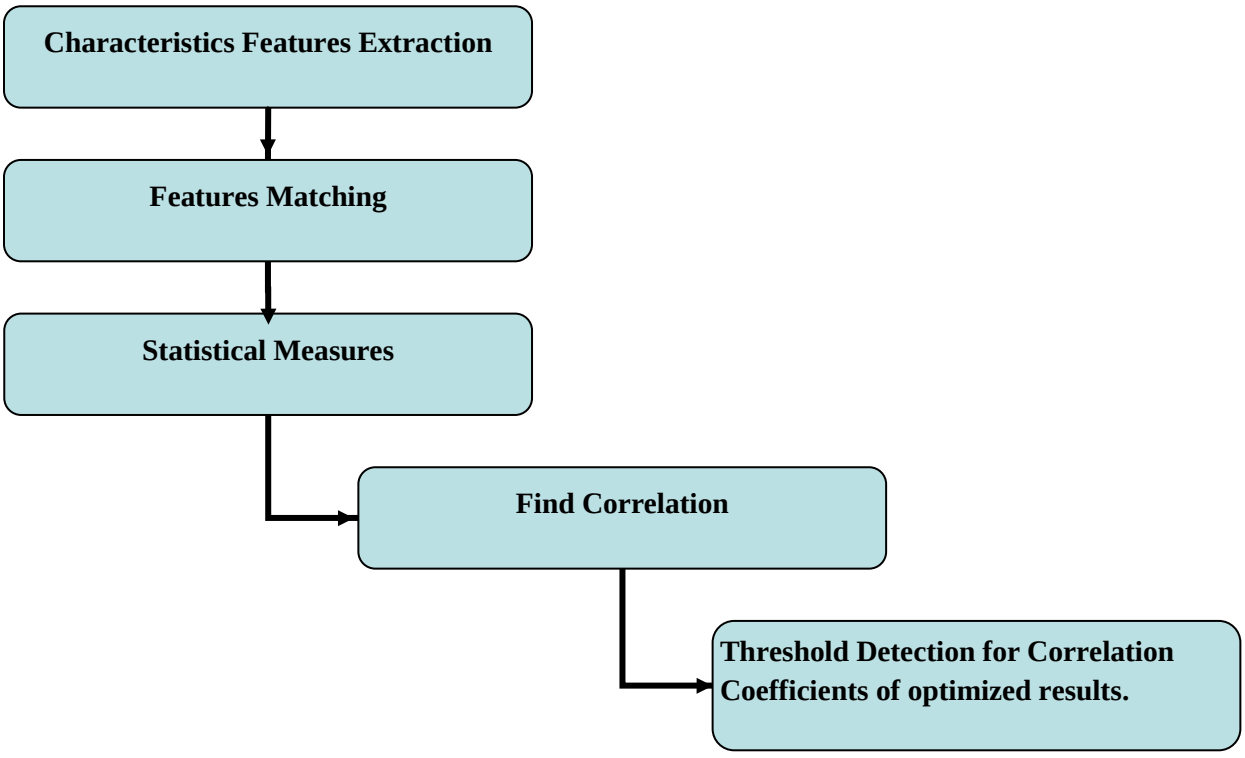

Figure 1: Digital Image Forgery Forensic Approaches

2. LITERATURE REVIEW

Forensic science investigation utilized in many applications for the purpose of security and authenticity of the original document. Various methodologies have been implemented by various researchers from last 20 years. Fridrich, Soukal and Lukas (2005) proposed an initiative to detect copy move forgery detection (CMFD) using block based approach through DCT. Many researchers used fridrich'paper as standard forgery detection for further literature but able to detect forgery in case of rotation up to 5 degree only. Various papers have been published every year to present CMFD as most active approach in image forensics. Existing methodologies from 2003 to till now uses the similar framework like divide the images of fixed size into overlapped blocks and apply feature extraction mechanism for extracting similarities among corresponding blocks.

Popescu and Farid (2005) proposed a blind approach using principle component analysis for forgery detection using different feature representation to obtain vector feature which was robust against compression attacks. Luo, Huang and Qiu (2006) used the same procedure by dividing image blocks into 4 subsets that is colour based sub-blocks division approach in simple forgery detection to shows robustness in compression only by using vector size of 1*7 and limited results in post processed images.

Mahdian and Saic (2007) employed moment of blur invariant approach for post processing forgery detection. Authors applied blurr moment only oncolour blocks having vector size of 1*72 and employed Principle Component Analysis (PCA) for reduced vector feature via K-tree to diagnose forged region of different size and shapes for dedicated interpolated images to perform resampled image operations. Kang et al. (2008) examined singular value decomposition over blocked images to get reduced dimensions so that robust results achieved against noise distortions.

Bayram, Sencar and Memon (2009) employed Fourier Mellin Transform with log polar 1D projection to get forged region localization in case of rotation attacks that is invariant in case of small regions. Authors employed bloom filters in matched process for speedup detection but have limitation over resized images. Lin et al. (2009) proposed block based feature extraction algorithm with average intensities. Ryu et al. (2010) employed Zernika moment for block based feature extraction and matching to obtained rotation as well as in pre rotated images which are invariant to rotation transformation.

Garfinkel (2010) presented an efficient review of digital forensic science research gives new directions of investigation. Authors included literature of coming 10 years started from 2010 was presented. Digital forensic is around 50 year old and initially required for data recovery from emails, data formatting, immediate deletion and identification, remedying data, software and hardware application, time sharing and centralized computing facilities. Therefore digital forensic is a very important part for many investigation like analysis of military, government organization and e-discovery. Digital forensic also helps in solving crime committed with computers like bank fraud, money laundering, and child exploitationary. Previous DFRWS and CDESF start together for digital evidences but due to inadequate resources group dispersed and HASS and CARVER support the digital forensic. Authors support XML representation of the data file. The authors also need to know how the digital forensic research can be more efficient by new concepts for data representation but only with the financial support which essential to accept criterions and processes for testing and validation of research products.The short- coming in their study includes-The lack of training and format incompatibility, Efficiency of available tools and research process reduces day by day and Examiners cannot get forensic data easily for processing.

Warbhe, Dharaskar and Thakare (2015) implemented a novel approach for cloning forgery detection via Normalized Cross Correlation. NCC is the tool for features matching in image registrations, tampering matching and pattern recognition. The authors uses coarse forgery detection for finding the highly correlated area where each uneven block act as template for NCC and fine-tuned detection for detecting forged region .NCC helps in computing the pixel based cross correlation normalized by auto correlation of the image. The authors use the block based method for forgery detection. This helps in finding the similarities and non-similarities of digital images in the range of +1 & -1. The various limitations of this study were need improved algorithms for post processing likes scaling, rotation, etc. and the threshold value is 0.98 for stet-size-4 and block size-20, which can be further improved by changing these two values.

Beek et al. (2015) presented data analysis for increased processing speed of forensic investigation with new technologies. The authors also explore the design principle like transparency, privacy and security with their implementations for business perspective. The authors uses some Forensic drivers for reducing the case lead time, maximum coverage of data, expert team analysis with the help of Hansen System. But Need to replace the Xiraf System by Hansen System.The authors tested different methodology like Data descriptions, Script platform, Feature Selection, Feature extraction, Colour derived feature similarities for the purpose of

reliability with the help of ROC which gives different evaluation metrics like True Positive Rate or False Positive Rate.

Kamenicky et al. (2016) presented different methods for video and image forensic analysis with their originality, increased image quality by reducing the noise, unwanted blur and other possible artifacts which helps in criminal investigation. The authors ensures the repetition of image analysis, image processing functionality like image source, their verification and restoration with the help of PIZZARO software. Authors represents tool for image forensic in three categories as1) Image source determination: Source device assignment, Detection in LCD re-captured images, Implementing Quantization includes: Image content verification: Double JPEG Compression, Interpolation detection, Copy move detection, Noise inconsistency, Chromatic aberration.3): Image restoration: DE-noising, Super –resolution, JPEG artifacts eliminations. The limitations in their study are as it is difficult to verify credibility, origin, image restoration by removing unwanted artifacts with increasing data quality, It is not time-effective in terms of the criminalist work facilitate and it is required to apply different methods to get stronger evidence.

Hitchcock, Le-Khac and Scanlon (2016) proposed method in which main objectives were to highly increase the efficiency of investigation of digital evidence timely by reducing backlog files for analysis in forensic laboratory.The authors' successfully implemented analysis between regular and non-regular forensic investigation. The authors also represents digital field triage analysis by planning, assessment, reporting, thresholdunder calculation of different phases like user account, crime type (internet activity, multimedia documents, software installed, emails), attached device, timely search and encryption, one by one. The digital field triage model work in two ways i.e. Digital Computer Field Triage and Digital Mobile Field Triage. The DFT members collect the confirmation from Ram memory running in that machine which meets the threshold for Technological crime unit examinations.The limitations in their study includes time consuming process between analysis of digital evidence and analytical report reception thereforeDFT members expertises required and advanced training required Ram capture, Basic Acquisition, Encoded capacity finding on real mechanism.DFT model's effectiveness and efficiency must be revised.

Hashmi, Hambarde and Keskar (2014) proposed an Effectual and Strong method for forgery detection through the process of feature extraction techniques called Dyadic Wavelet Transform using Scale Invariant Feature Transform that helps in detecting large key points matching.Experimental results shows that using SIFT the Precision was 95% but with combined efforts of DYWT +SIFTS, Precision was 88% with the False Positive Rate of 10%.

Amerini et al. (2013) presented Image Forensics shows authenticity of digital images can easily be detected and can be utilized as proof for judgment. Authors projected different procedure based on scale invariant features transform for splicing, cloning occurrence and recovering the geometric transformation for cloning with high reliability. The major drawback is how to improve investigation of cloned damage patch with highly uniform texture and how to extend clustering phase by image segmentation procedure.

Stamm (2010) proposed an efficient and effective method for detecting contrast enhancement with the help of intrinsic fingerprint where the noise is added before JPEG compression .The authors also tested many simulations for detecting their designated image processing processes with the prospect of detection and probability of false alarm is only 7%.The major disadvantages include additive noise need to be improved using enhanced methodology.JPEG compression in discrete cosine transform (DCT) field with the image quality shows the enhanced trade-off among the JPEG Anti- forensic delectability and visual eminence of examined images which different double JPEG compression artifacts as suggested.

Fan, Wang, Cayre and Xiong (2014) Proposed JPEG forgery process involve: TV based DE blocking, DCT histogram, DE calibrations. Multiple cloned forgery detection with different domains at same time provides good image resolution through PSNR and SSIM metrics. Authors proposed JPEG anti forensic techniques gives compromise between quality of images and detection speed. The major limitations of their studies include designing the optimal techniques for multiple forgery detection using JPEG non-convex SSIM metric, need to have a better histogram restoration for different image DCT statistics design implementation for anti-forensics and hard optimization required for SSIM non-convex imaging.The proposed methodology for the forensic investigation implemented on inside and outside acquisition devices for post operations to verify integrity of digital image forensics, which helps in computing inverse Filter Coefficients by Constrained Optimization. “JPEG compression has been considered as quantization in the discrete cosine transform (DCT) domain and statistical analysis”

Swaminathan, Wu and Liu (2008) proposed methodology for Post camera processing of Steganography Embedding and Watermarking and estimated filter coefficients for splicing forgery detection. Arthur’s shows inconsistencies in fingerprints results regardless of input source images like scanner, or computer graphics software. Proposed methodology also applicable for direct camera results. The major limitations of their study are tampered detection for received image characteristics shows average accuracy of 62% and 52% at the rates of 100% and 78%, respectively and average identification accuracy is reduces to 91%.

Tang, Kong and Craft (2011) Proposed algorithm that affects the visibility of blocks in skin images and Recognizing individuals in indication images and JPEG-compressed kid pornography is very common. Proposed knowledge-based approach eliminates JPEG obstructive artifacts and improves skin key- features through different algorithms like: Markov-model and faster algorithm. Block synthesis algorithm for different cases not good for input blocks contained in the training set. The visual quality of biometric features is also improved. Authors also designed an indexing mechanism for speed up these algorithms.The short- coming in their study having-Complexity is extremely high in iterative process of forward and inverse DCT calculations of tested images and compressed image quality factor reduced only up to 50, average compressed ratio was only 72.55, as number of images increased the compression quality factor reduced by half and the average compression ratio was reduced respectively.

Swaminathan, Wu and Liu (2007) proposed visual sensors methodology for estimation of colour filter array and interpolations. Authors' analysis shows similar features by different methodologies applied over different camera model for licensed potential infringement. Proposed methodology includes: Testing Of Objects, Features Extraction, Classification, Testing and Validation. It is also good for the post processing. But major limitation is that it having only 90% average accuracy for efficiently identifies the correct camera brand. Investigation of inside components of digital cameras like data sensors and white balanced give beneficial data for dissimilar features of the sensors.

Grier and Richard (2015) proposed algorithms for acquisition and disk management via imaging systems. Results show the acceleration more than 3 for collected evidence of 95%. The limitation of their studies is to test the sifting collectors requires library expanding profiles and need of strong analysis for post operation of different format of images for integrating purpose.

Warbhe, Dharaskar and Thakare (2016) proposed novel approach for copy past detection by Normalized Cross Correlation Image editing software programs makes manipulations very easily like copy past ,composing, splicing. Passive forgery detection includes block based or key-point methods for forgery detection. Authors uses Discrete Cosine transform (DCT) approach for cost reduction with the help of Fine-Tuned Scale Tampering detection and Coarse Scale Tampering Detection.The major limitations of their studies are to find exact tampering size area for detecting forged region and rotation angle.

Malviya and Ladhake (2016) presented blind Image Forensics for detecting forgeries like scaled, rotate, translate and cloning images with new approach Auto Colour Correlogram features extraction technique to detect multiple cloning in the same image. Proposed work includes: noise

filtering, transformation, auto colour correlogram for feature extraction, matching similarities for forgery detection. Result shows Precision by ACC is only 95.65% with FPR of 16 and FNR of 32 by testing 400 database images.

Ustubioglu, Ulutas, Ulutas and Nabiyev (2016) proposed forgery detection methods using Benford's generalized Law and Discrete cosine transform to achieve limited feature vectors helps to obtain optimized threshold value automatically which robust for all post processing operations .Authors proposed higher accuracy ratio and lower FN value only up to p=0.99 and f=0.04. Bi and Pun (2018) presented feature correspondences using enhanced coherency sensitive hashing and local bidirectional coherency error to get sensitive results via multiple iterative process to decide specified threshold to achieve fast detection for real time effectiveness with final measure up to 96.63%.,which needs further improvements.

Table1. Comparative Analysis of Existing Forensic Image Approaches

Feature Extraction Techniques	Precision%	Recall %	Score%
discrete cosine transform (DCT)	78.69	100	88.07
principal component analysis (PCA)	84.21	100	93.20
DyWT +SIFT	88	80	83.80
knowledge-based (KB) approach	90.1	90	90.05
Speed Up Robust Features (SURF)	91.49	89.58	90.53
Normalized Cross Correlation (NCC)	94	90	91.95
Scale invariant features transform (SIFT)	95	74	83.20
Auto Colour Correlogram (ACC)	95.65	91.67	93.62

2.1 Gaps in Literature

1. Computational complexity in terms of time and space are very high.
2. Need of forgery detection speed improvement especially in small tampered regions.
3. Statistical measurement analysis for image integrity is difficult due to similar component used in forged region, compatible with rest of the images.
4. Image forgery is very simple due to the powerful computer programmed software like Adobe Photoshop, Corel Paint Photoshop and these images editing tools are available easily from free online resources at any time for the purpose of image manipulations.
5. Testing procedure will be difficult for massive amount of data manually which need to automatic for authenticresults.
6. Need to develop a robust algorithm which must be tested for all the transform techniques to give commendable results.

3. DESCRIPTION OF BROAD AREA

Images are very important part of our daily life routine for communicating effective idea where human eye and brain mechanism gives imaging system as first scene is recorded by the eye and brain processed it and give some meaningful information for image analysis. Image sources may be through the pictures, painting, newspaper, TV and Internet and digital libraries. Digital image processing involves improvement in the field of human interpretation about picture data, manipulation of image data and their processing for storage and transmission. It gives the scope of digital image processing via digital computers so that the post processing becomes easy with small corrections. As image processing is the manipulation of images done by computer programmes where an object is captured by camera and information extracted from computers for further processing. Forensic science now utilized in various organizationsfor their internal document management like trash mails records, email record maintenance with continuous analysis of all active and passive activities of their employee's.

Forensic image application process includes the fingerprint identification, facts to identify criminals, industrial applications and remote sense applications. Forensic investigation works on quality of image data and their restoration by reducing unwanted blur, noise etc. Table1. Represents comparative analysis of existing forensic image approaches and Table2. Highlights the proposed frame work of the research. Figure2. includes Digital Image Processing approaches in different phases like Image Acquisition, 2-D signal (image), Spatial Domain, Frequency Domain, Image Enhancement, Image Restoration, Image Segmentation, Object Recognition, Image Compression, Binary Image Processing, Colour Image Processing and Wavelet based Image Processing, each explained as following (Birajdar and Mankar 2013; Garfinkel 2010).

Image Acquisition: It is the process of capturing real images and stores them in computer system. Digital cameras capture images directly in digital form using CCD or CMOS image sensors.2-D signal (image): Intensity of image can varied in x and y directions called 2-D signal (image).System act as operations performed on input signal to produce output signal like 2D discrete signal presented as x(n1,n2), where n1,n2 are pair of integers and x act as real or complex value. In an image x(n1,n2) presents pixel intensity at location (n1,n2).Spatial Domain includes correlation and convolution operations to extract information from images. They are the linear (Pixel is replaced by linear combination of its neighbours) and sift invariant (Same operation is performed at every point in the images).

Frequency Domain: Image transform used in image processing and image analysis to move from time domain to frequency domain for fast computation convolution and correlation. Transform plays important role in various image processing applications like Image analysis, Image filtering, Image enhancement and Image compression. Transform having sinusoidal as basis functions called Fourier Transform. Transform having non- sinusoidal as basic functions called Haar- Transform (simplest), Walsh Transform, Hadamard- Transform and slant Transform. In wavelet Transform images can be represented in different resolutions. Transform whose basic function depends on statistics of input signal are KL Transform (best linear Transform in terms of energy compaction) and Singular Value Decomposition. Transform which represents directional information of an image signal includes Hough Transform, Radon Transform, Ridgelet Transform, Contourlet Transform.

Image Enhancement: It is used to improve the quality of an image by suppressing noise, increasing image contrast, image emphasise and sharpen/smoothen image. Image Restoration: It is used to reconstruct original scene from a degraded one by linear frequency distortion, noise, blocking artifact like deterministic blur (motion, defocusing, atmospheric turbulence) and random noise.Image Segmentation: Main objective of Image Segmentation is to extract various features of images which merged or split for analysis and interpretation and pattern recognition. Segmentation split image in to connected areas in order to divide image in to meaningful regions. Object Recognition: It is an attempt to distinguish different objects in an image. It helps in recognition of objects with in a fraction of seconds.

Image Compression: It is very important in many multimedia applications like Image storage and transmission. It is a mapping from a higher dimensional space to a lower dimensional space. Basic aim is to represent an image with minimum number of bits of an acceptable image quality. It removes statistical redundancy and exploit perceptual irrelevancy while reducing data as much as possible.Binary Image Processing: It includes different operations like morphology and nonlinear process to remove details smaller than a certain reference shape. It is used to extract the edges of an image, filter an image and skeletonises an image etc.

Colour Image Processing: It uses physiology of colour perception used to distinguish object, material, place and time. It occupies more space when compared to gray scale and binary images. To understand colour we need to understand the nature of light like colour information, colour model CIE chromatin, colour quantisation, colour histogram equalisation, colour image filtering and colour pseudo colouring.

Wavelet based Image Processing: Wavelet transform is a tool to allow multi resolution analysis of an image to extract relevant information from an image.It presents application in field of an image compression, image de-noising and image watermarking.To understand wavelet need to know about linear algebra and signal processing.

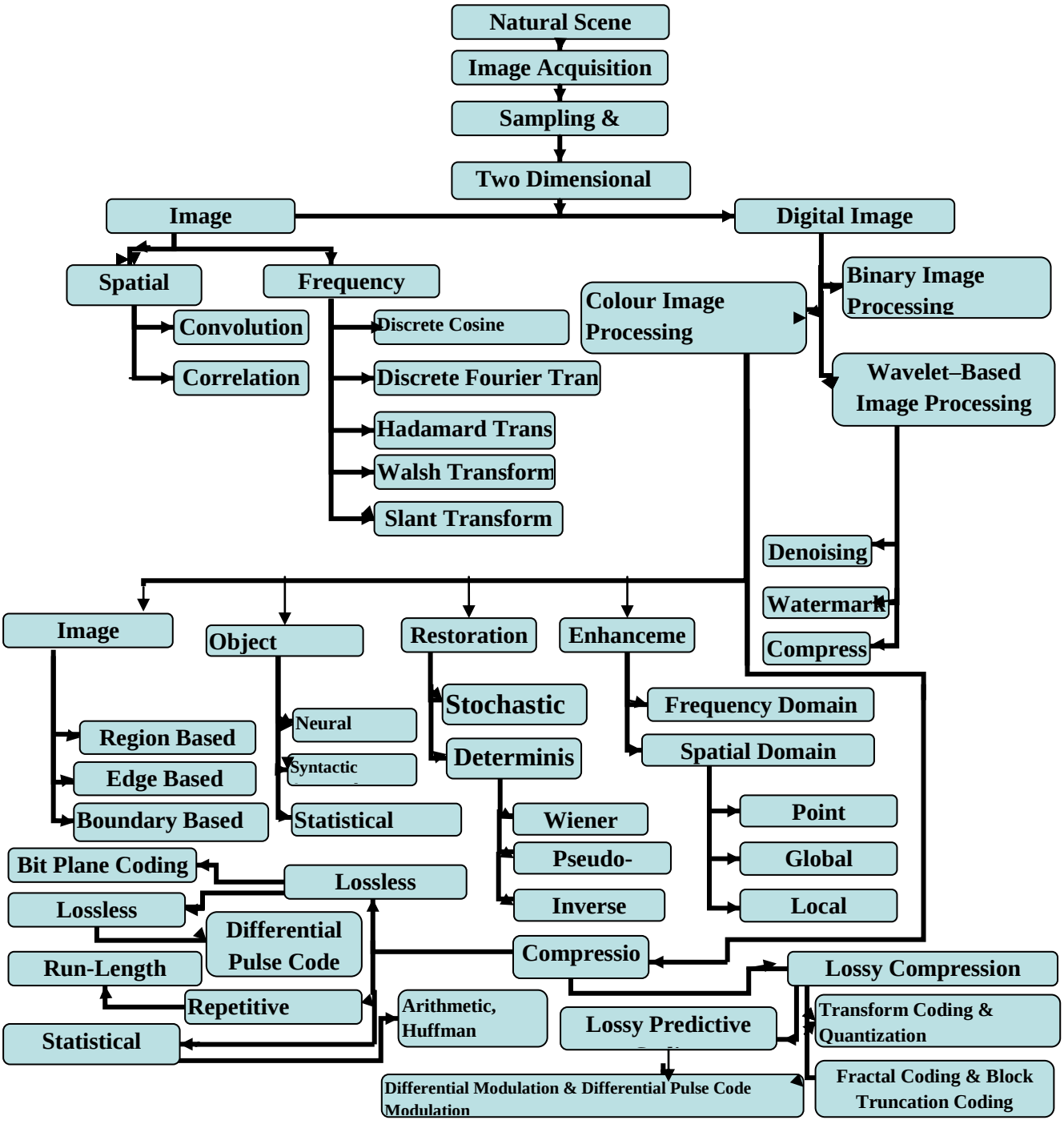

Figure2. Digital Image Processing Approaches

3.1DIFFERENT IMAGE TRANSFORMATION TECHNIQUES

Transform techniques are an important tool for image processing which shows results in time and frequency domain. Following different transform techniques are applied over digital images to get better results which show inconsistent output in every condition of forgeries.

Principle Component Analysis (PCA): PCA helps in generating orthogonal axis of projections called principle components (Eigen vectors) of input for decreasing variance. In this Eigen vector of covariance matrix forms KL transform called Principle Component Analysis or Hotelling transform. With the help of Principle Component Analysis original images can be transformed in to corresponding Eigen face for finding the image originality.

Signal value Decomposition (SVD): SVD approach can be used in image compression, face recognition, watermarking and texture classification.

Fourier Mellin Transform (FMT): FMT used in content based image processing, digital watermarking, patternrecognition and speech signal analysis. It is used to extract features that can be invariant to shifting, scaling, rotation and translation can be found in different locations, scales and orientations.

Discrete Cosine Transform (DCT): DCT is a technique to convert signal into elementary frequency components and widely used in image compression. DCT has excellent energy compaction for highly correlated data. Separable property of 2D-DCT helps in computing image by successive 1D operation on rows and columns of an image.

Polar Cosine Transform (PCT): It is used to obtain the invariant patterns for 2D images by extracting rotation invariant image patterns. It can transform image function to mutually independent patterns with maximum discriminated information and minimum redundancy.

Discrete Wavelet Transform (DWT): It transforms a discrete time signal to a discrete wavelet representation. It is an implementation of wavelet transform with the help of combination of discrete set of wavelet scales and translations. It provides inherent multi resolution nature, wavelet coding for scalability. DWT is also used for compression, watermarking, etc. It is not shift invariant therefore a simple shift can cause a significant energy in DWT coefficients.

Walsh Transform: It introduced a set of orthonormal square wave functions. It is computationally simple as Walsh functions are real and they take only two values ie +1 or -1.Hadamard Transform: It is same as Walsh Transform except rows of transform matrix are reordered. Elements are mutually orthonormal ie +1 or -1 for producing low computational complexity in calculation of transform coefficients.Hadamard Transform: It is based on

orthogonal matrices whose elements are +1 or -1, multiplied by powers of 2.It is computationally efficient transform as transform of n points vector requires only 2(n-1) addition and n multiplications.

Scalar Invariant Feature Transform (SIFT): It is an algorithm helps in describing local features in digital images. It locates certain key-points called descriptors for object recognition and these descriptors are invariant against various transformations. It is used for detecting salient and stable feature points from an image. It helps for image estimation of affine transformation between images. SIFT features are not changed with object position, scale, illumination, image artifacts, noise and blur.

Speedup Robust Feature Transform (SRFT): It is a local feature detector descriptor used for object recognition, image registrations and classification. It is much faster transform algorithm which uses integer approximation of hessian blob detector and having descriptor sum of haar wavelet response around point of interest. It used square shaped filters for Gaussian smoothing.

3.2APPLICATIONS OF FORENSIC IMAGE INVESTIGATION

It includes Forensic Investigation, Criminal Investigation, Surveillance Systems, Intelligence Servicesand Medical Imaging Journalism etc .Forensic techniques used in specific field like image analysis which helps in providing sequence of events and focuses on prevention of future misuses. Main aim is to determine image enhancement for maximum information extraction.

4. OBJECTIVES OF THE STUDY

4.1 Problem Formulation Statement:-

Improvisationis needed in forgery detection over multiple cloned objects with identical consistency where salient key-point features are difficult to recover. Improvement of forgery detection speed is the main concern with the implementation of reduced computational complexity. Accuracy and efficiency of image forensic investigationwill be tested throughvarioustransform techniques for consistent results. Testing requires to be applied on different formats of digital images in order to get better results.

4.2 Objectives:-

1. To collect forged image dataset from online resources like MICC_F220, MICC_F600 etc.

2. To test forged images using various existing transform techniques for originality.
3. To identify exact location of forgery and analyse evaluation parameters.
4. To develop novel algorithms for optimizing forensic science investigation.
5. To implement the findings on real time datasets.

5. METHODOLOGY TO BE ADOPTED

The proposed work would be obtained based on following phases:

Phase1: Literature survey and related work done in respect of different techniques for Designing, implementation and analysis of Image forensic investigation.

Phase2: Study of available tools, mechanisms, categorizing issues and challenges, evaluating disadvantages of existing protocols and identifying areas of improvisations.

Phase3: Digital database collection. Images shall be collected from MICC_F220 database and real-time signals would also be collected.

Phase4: Formulating the research objectives- The Problem statement Implementation-to achieve research objectives by MAT LAB software tools and apply optimization techniques to identify the best image investigation methods for authentication of the images.

Phase5: Paper presentation and publications based on the research work.Finally report writing, reviewing of thesis and submission.

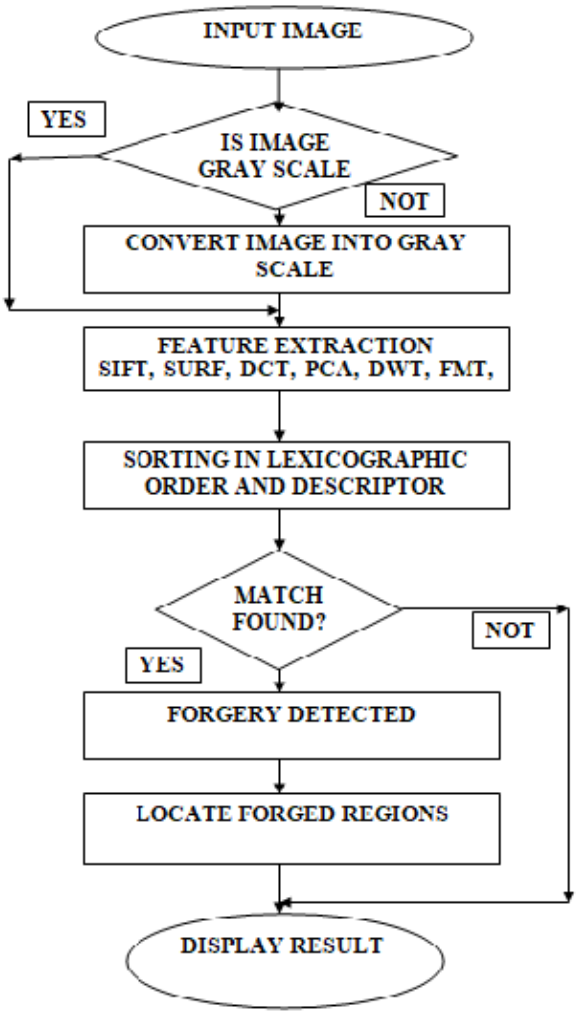

Figure3. Work Flow Chart for research design methodologies.

5.1 EVALUATION PARAMETERS

1. False Positive Rate(FPR) = False Positive / True Negative + False Positive
2. False Negative Rate (FNR) = False Positive / True Positive + False Positive
3. Sensitivity(TPR) = True Positive / True Positive + False Negative
4. Specificity(TNR) = True Negative / True Negative + False Positive
5. Precision = True Positive / True Positive + False Positive
6. Accuracy = True Positive + True Negative / True Positive + True Negative + False Positive+ False Negative
7. Final score =2 True Positive / 2 True Positive + False Positive + False Negative

6. EXPECTED OUTCOME OF THE RESEARCH

1. Forensic Investigation of digital images will be evaluated based on various parameters for artefact removal from tampered images and compared with recent existing techniques.
2. Image forgery detection algorithm will be developed for providing Quality of Services like Security, Accuracy, Reliability, computational complexity and real time implementations.

7. Proposed Time Frame

The research work has been divided into various tasks and they will be achieved on the basis of the time lines mentioned in the Gantt chart shown below

Table2. Proposed Time Frame Work

Time Frame →	**Jan-Jun 2017**			**July-Dec2017**			**Jan-Jun2018**			**July-Dec2018**			**Jan-Jun2019**			**July-Dec2019**			**Jan-Jun2020**		
Months	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42
Course Work																					
Extensive Literature Search																					
Problem Statement Formulation																					
Publication on Literature Survey																					
Analyze the effect of various transforms techniques for artifact removal in digital forgeries.Examine the existing work.																					
Publication on Digital forgeries detection to eliminate any type of tampering																					
Study of special structure under different level of forgeries																					
Algorithm development to identify effect of various forgeries on digital images																					
Publication on forensic forgeries detectionReport writing & Submission																					

REFERENCES

Al-Qershi, O. M., &Khoo, B. E. (2013). Passive detection of copy-move forgery in digital images: State-of-the-art. *Forensic Science International*, 231(1–3), 284–295

Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Del Tongo, L., & Serra, G. (2013).Copy-move forgery detection and localization by means of robust clustering with J-Linkage.*Signal Processing: Image Communication*.

Amtullah, S., &Koul, D. A. (2014). Passive Image Forensic Method to detect Copy Move Forgery in Digital Images. *IOSR Journal of Computer Engineering*, *16*(2), 96–104.

Bashir, T., Usman, I., Khan, S., &Rehman, J. (2017). Intelligent reorganized discrete cosine transform for reduced reference image quality assessment. *Turkish Journal of Electrical Engineering & Computer Sciences*, 1–25.

Bayram, S., Sencar, H., &Memon, N., (2009).An Efficient and Robust Method for Detecting Copy-Move Forgery.*IEEE International Conference on Acoustics, Speech, and Signal Processing*, 1053–1056.

Bi, X., & Pun, C. (2018).Fast Copy-Move Forgery Detection Using Local Bidi- rectional Coherency Error Refinement.*Pattern Recognition*, (18), 1-38.

Birajdar, G. K., & Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. *Digital Investigation*, *10*(3), 226–245.

Chauhan, D., Kasat, D., Jain, S., & Thakare, V. (2016).Survey on Keypoint Based Copy-move Forgery Detection Methods on Image.*Procedia Computer Science*, *85*(Cms), 206–212.

Chu, X., Member, S., Chen, Y., Stamm, M. C., & Liu, K. J. R. (2016).Information Theoretical Limit of Operation Forensics.*IEEE Trans. Information Forensics and Security*, *11*(4), 774–788.

Dietrich, D., &Adelstein, F. (2015).Archival science, digital forensics, and new media art.*Digital Investigation*, *14*(S1), S137–S145.

El-Alfy, E. S. M., &Qureshi, M. A. (2015). Combining spatial and DCT based Markov features for enhanced blind detection of image splicing. *Pattern Analysis and Applications*, *18*(3), 713–723.

Fan, W., Wang, K., Cayre, F., &Xiong, Z. (2014).JPEG anti-forensics with improved tradeoff between forensic undetectability and image quality.*IEEE Transactions on Information Forensics and Security*, *9*(8), 1211–1226.

Franklin, D., Swift, L., &Flavel, A. (2016).“Virtual anthropology” and radiographic imaging in the Forensic Medical Sciences.*Egyptian Journal of Forensic Sciences*, *6*(2), 31–43.

Fridrich, J., Soukal, D., & Lukas, J., (2003). Detection of copy-move forgery in digital images. *Digital Forensic Research Workshop (DFRWS), Cleveland, USA*, 134–137.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*(SUPPL.).

Gherghel, S., Morgan, R. M., Blackman, C. S., Karu, K., & Parkin, I. P. (2016).Analysis of transferred fragrance and its forensic implications.*Science and Justice, 56*(6), 413–420.

Grier, J., & Richard, G. G. (2015).Rapid forensic imaging of large disks with sifting collectors.*Digital Investigation*, *14*, S34–S44.

Guido, M., Buttner, J., & Grover, J. (2016).Rapid differential forensic imaging of mobile devices.*Digital Investigation*, *18*, S46–S54.

Hashmi, M. F., Anand, V., &Keskar, A. G. (2014). Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform. *AASRI Procedia*, *9*(Csp), 84–91.

Hashmi, M. F., Hambarde, A. R., &Keskar, A. G. (2014). Copy move forgery detection using DWT and SIFT features. *International Conference on Intelligent Systems Design and Applications, ISDA*, 188–193.

Hitchcock,B., Le-Khac.N., & Scanlon.M. (2016). Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists. *Digital Investigation,(16)* .S75-S85.

Kamenicky, Jan.,Bartos, Michal.,Flusser, Jan.,Mahdian,Babak.,Kotera, Jan.,Novozamsky, Adam.,Saic,Stanislav.,Sroubek,Filip.,Sorel,Michal.,Zita,Ales.,Zitova,Barbara.,Sima,Zdenek., Svarc, Petr., & Horinek, Jan. (2016). Forensic analysis and restoration of image and video data.*International Journal of computer applications.* 264, pp.153–166.

Li, J., Li, X., Yang, B., & Sun, X. (2015).Segmentation-based image copy-move forgery detection scheme.*IEEE Transactions on Information Forensics and Security*, *10*(3), 507–518.

Lin Z., He J., Tang X., & Tang C. (2009b). Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis. *Pattern Recognit* .42(11), 2492–2501.

Luo W., Huang J., &Qiu G. (2006).Robust detection of region-duplication forgery in digital image.*Proc. of the 18th International conference on pattern recognition recognition,* 746–749

Mahdian, B., &Saic, S., (2007). Detection of copy-move forgery using a method based on blur moment invariants. *Forensic Sci. Int,* 180–189.

Malviya, A. V, & Ladhake, S. A. (2016). Pixel based Image Forensic Technique for copy-move forgery detection using Auto ColorCorrelogram .*Procedia - Procedia Computer Science*, *79*, 383–390.

PopescuAC., &Farid H. (2005).Exposing digital forgeries by detecting traces of resampling. *IEEE Trans Signal Process*.53(2),758–767.

Prasad, S., &Ramkumar, B. (2017). Passive copy-move forgery detection using SIFT, HOG and SURF features. *2016 IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016 - Proceedings*, 706–710.

Qureshi, M. A., &Deriche, M. (2015).A bibliography of pixel-based blind image forgery detection techniques.*Signal Processing: Image Communication*, *39*, 46–74.

Raj, R., & Joseph, N. (2016).Keypoint Extraction Using SURF Algorithm for CMFD.*Procedia Computer Science*, *93*(September), 375–381.

Rocha, A., Scheirer, W., Boult, T., &Goldenstein, S. (2011).Vision of the unseen.*ACM Computing Surveys*, *43*(4), 1–42.

Ryu., S.-jin., Lee, M.-jeong., & Lee., H.-kyu., (2010).Detection of copy-rotate-move forgery using zernike moments.*Information Hiding. LNCS* 6387, (1), 51–65.

Silva, E., Carvalho, T., Ferreira, A., & Rocha, A. (2015).Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes.*Journal of Visual Communication and Image Representation*, *29*, 16–32.

Sitara, K., &Mehtre, B. M. (2016). Digital video tampering detection: An overview of passive techniques. *Digital Investigation*, *18*, 8–22.

Stamm, M. C., & Liu, K. J. R. (2010).Forensic detection of image manipulation using statistical intrinsic fingerprints.*IEEE Transactions on Information Forensics and Security*, *5*(3), 492–506.

Stamm, M. C., & Liu, K. J. R. (2011).Anti-forensics of digital image compression.*IEEE Transactions on Information Forensics and Security*, *6*(3 PART 2), 1050–1065.

Swaminathan, A., Wu, M., & Liu, K. J. R. (2007). Nonintrusive component forensics of visual sensors using output images. *IEEE Transactions on Information Forensics and Security*, *2*(1), 91–105.

Swaminathan, A., Wu, M., & Liu, K. J. R. (2008).Digital image forensics via intrinsic fingerprints.*IEEE Transactions on Information Forensics and Security*, *3*(1), 101–117.

Tang, C., Kong, A. W. K., & Craft, N. (2011).Using a knowledge-based approach to remove blocking artifacts in skin images for forensic analysis.*IEEE Transactions on Information Forensics and Security*, *6*(3 PART 2), 1038–1049.

Ulutas, G., Ustubioglu, A., Ustubioglu, B., V. Nabiyev, V., &Ulutas, M. (2017).Medical Image Tamper Detection Based on Passive Image Authentication.*Journal of Digital Imaging*, 1–15.

Ustubioglu, B., Ulutas, G., Ulutas, M., &Nabiyev, V. V. (2016). A new copy move forgery detection technique with automatic threshold determination. *AEU - International Journal of Electronics and Communications*, *70*(8), 1076–1087.

Vaid, A. K. (2016). Survey of Forensic and Analysis Tools based on Grouping of Digital Evidence using Metadata Functionality. *International Journal of computer application*, *142*(3), 28–35.

Van Beek, H. M. A., Van Eijk, E. J., Van Baar, R. B., Ugen, M., Bodde, J. N. C., &Siemelink, A. J. (2015). Digital forensics as a service: Game on. *Digital Investigation*, *15*, 20–38.

Warbhe, A. D., Dharaskar, R. V., & Thakare, V. M. (2015). A Scaling Robust Copy-Paste Tampering Detection for Digital Image Forensics. *Procedia - Procedia Computer Science*, *79*, 458–465.

Warbhe, A. D., Dharaskar, R. V., & Thakare, V. M. (2016).A Survey on Keypoint Based Copy-paste Forgery Detection Techniques.*Physics Procedia*, *78*(December 2015), 61–67.

Warbhe, A. D., Dharaskar, R. V., & Thakare, V. M. (2016).Computationally Efficient Digital Image Forensic Method for Image Authentication.*Procedia Computer Science*, *78*(December 2015), 464–470.

Warif, N. B. A., Wahab, A. W. A., Idris, M. Y. I., Salleh, R., & Othman, F. (2017). SIFT-Symmetry: A robust detection method for copy-move forgery with reflection attack. *Journal of Visual Communication and Image Representation*, *46*, 219–232.

Zandi, M., Mahmoudi-Aznaveh, A., &Talebpour, A. (2016).Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector.*IEEE Transactions on Information Forensics and Security*, *11*(11), 2499–2512.